Fact Sheet: Enterprise Architecture Framework, Version 2.0 for the Information Sharing Environment

---

"Today, the sharing of terrorism-related information takes place within multiple independent sharing environments that serve five communities – intelligence, law enforcement, defense, homeland security, and foreign affairs. Historically each community developed is own policies, rules, standards, architectures, and systems to channel information to meet mission requirements. These environments were insulated from one another, which resulted in gaps . . . Our objective is to establish a framework for federal agencies in the fulfillment of their individual roles and responsibilities and forge a coordinated and trusted interagency partnership and process across all five communities."

– National Strategy for Information Sharing, October 2007

Enterprise Architecture Framework Updated With New Business Processes

- On September 30, 2008, Ambassador Thomas E. McNamara, Program Manager for the Information Sharing Environment (PM-ISE), released the second version of the *Information Sharing Environment (ISE) Enterprise Architecture Framework (EAF)*.
- This newest version of the *ISE EAF*, was developed through a collaborative process involving the Information Sharing Council (ISC), and builds on the foundation established in Version 1.0 to provide more specificity and granularity for ISE business mission processes and information flows.
- The *ISE EAF Version 2.0* provides guidance at a level of detail greater than that provided by the Federal Enterprise Architecture Framework (FEAF), and assists individual agencies as they adapt their enterprise architectures, and especially their Information Sharing Segment Architectures (ISSA), in order to implement the ISE.
- New additions in Version 2.0 of the *ISE EAF* include:
    - Greater granularity to support the mission business processes for:
        - Suspicious Activity Reporting (SAR),
        - Identification and Screening (Terrorist Watchlist components), and
        - Alerts, Warning, and Notification (AWN);
    - The roles and responsibilities of the ISE Implementation Agents for implementation within the ISE Core;
    - ISE Shared Spaces components discussion;
    - An ISE Identity and Access Management (IdAM) Framework; and
    - A cross mapping of ISE business mission processes to the Federal Enterprise Architecture (FEA) Business Reference Model (BRM) sub functions.

Background on the ISE Enterprise Architecture Framework

- The *ISE EAF* addresses key requirements of *The Intelligence Reform and Terrorism Prevention Act of 2004* and provides implementation guidance to ISE participants:
  - It builds on existing policies, business processes, and technologies in use by Federal, State, local and tribal governments that support information sharing within the law enforcement, homeland security, intelligence, foreign affairs, and defense communities, in a manner that fully protects the information privacy and other legal rights of Americans;
  - It provides a roadmap to enable long-term technology improvement and information systems planning, investing, and integration to support the sharing of terrorism-related information; and
  - Identifies and establishes the interfaces and standards needed to facilitate information sharing.
- PM-ISE and the Office of Management and Budget (OMB) oversee implementation of the *ISE EAF* through reviews and assessments and will update it as needed.
  - The *ISE EAF* is being incorporated into the Federal Enterprise Architecture (FEA), the Enterprise Architectures of ISC members, and the National Communications System *Continuity Communications Architecture*.
  - ISE participants incorporate the *EAF* attributes into their capital planning and investment control processes and overarching FEA Assessments for OMB.
- Enterprise architectures help organizations align resources to internal mission and strategic goals and priorities. The *ISE EAF* references the established ISE performance goals to provide ISE participants a common strategic vision to align their performance management efforts with defined desired results for the ISE. The *ISE EAF* also outlines the business processes, information flows and relationships, services, high-level data descriptions and exchanges, to include:
  - ISE Core Services – discovery (e.g. search and metadata registration), security (e.g. authentication and appropriate access control), mediation, messaging, collaboration, enterprise security management, and storage (e.g. directory services);
  - ISE Portal Services - collaboration, user interface, portal hosting, publish/subscribe, and user assistance; and
  - ISE Core Transport to connect agencies at designated interfaces for supporting information sharing.
- *ISE EAF* is comprised of four components:
  - Business Partition - identifies the performance drivers and desired outcomes, business functions, processes and information flows that support the ISE.
  - Data Partition - identifies and describes the data required to support the ISE business processes through the functional standards of the Common Terrorism Information Sharing Standards (CTISS) program.

  - Application and Service Partition - describes the software applications and service components that support the business processes.
  - Technical Partition - identifies the technologies and CTISS technical standards to be used to implement the applications and services.

BACKGROUND ON THE INFORMATION SHARING ENVIRONMENT

- Section 1016 of the *Intelligence Reform and Terrorism Prevention Act of 2004* calls for the development of an ISE to facilitate the sharing of terrorism and homeland security information among Federal, State, local, and tribal governments and, as appropriate, foreign governments and the private sector.
- As a part of implementing the ISE, the law requires the PM-ISE to describe the functions, capabilities, resources, and conceptual design of the ISE, and the impact on the enterprise architectures of participating agencies. The EAF supports these requirements.
- The Information Sharing Council was called for by the *Intelligence Reform and Terrorism Prevention Act of 2004* and established by Executive Order 13388 to advise the President and the Program Manager, Information Sharing Environment, and to provide for coordination among the federal agencies participating in the ISE.